УДК 640:004.78-049.5

Зябкин В.С., Бабенко А.А.

ОЦЕНКА ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ В ОРГАНИЗАЦИИ КОММУНАЛЬНОГО ХОЗЯЙСТВА

Аннотация. В настоящее время различные организации коммунального комплекса внедряют технологии автоматизации управления производственными процессами. В связи с этим актуальны вопросы обеспечения надежного, безаварийного функционирования автоматизированной системы управления технологическими процессами (АСУ ТП) и ее информационной безопасности (ИБ). Цель – провести исследование механизма оценки информационной безопасности автоматизированной системы управления технологическими процессами на предприятии коммунального комплекса г. Волгограда. Задачи: раскрыть сущность и особенности безопасности АСУ ТП; сформулировать алгоритм оценки защищенности АСУ ТП организации коммунального комплекса; разработать программный комплекс и провести экспериментальные испытания. В результате авторами установлены потенциальные угрозы информационной безопасности АСУ ТП ООО «Концессии водоснабжения» г. Волгограда и предложены методы повышения защищенности от основных видов атак, направленных на ИБ АСУ ТП. Предложена формальная модель оценки защищенности ИБ АСУ ТП организации коммунального комплекса. В разработанной модели используется системы защиты с полным перекрытием, в которой рассматривается взаимодействие «области угроз», «защищаемой области» (ресурсов АСУ ТП) и «системы защиты» (механизмов безопасности АСУ ТП). Предложенная модель позволяет решить задачу повышения защищенности АСУ ТП организации коммунального комплекса. Разработана архитектура программного комплекса оценки защищенности АСУ ТП организации коммунального комплекса. Представлен интерфейс, блок-схемы алгоритмов разработанного программного комплекса. Разработанный программный комплекс прошел тестовые испытания на предприятии ООО «Концессии водоснабжения».

Ключевые слова: информационная безопасность, информационные угрозы, АСУ ТП, механизмы защиты, анализ защищенности, оценка защищенности.

Abstract. Currently, various organizations of the communal complex are introducing technologies to automate the management of production processes. In this connection, the issues on the agenda include the provision of reliable, trouble-free operation of the automated process control system (APCS) and its information security (IS). The purpose of the article is to conduct a study of the mechanism for assessing the IS of an APCS at a public utility complex in Volgograd. Tasks: to reveal the essence and safety features of the automated process control system; formulate the algorithm for assessing the security of the automated process control system of the communal complex; develop a software package and conduct experimental tests. As a result of the in-depth analysis, the authors has established the potential threats to the information security of the automated process control system of the enterprise under study (LLC «Kontsessii vodosnabzheniya») and suggested methods for increasing security against the main types of attacks directed at APCS. The authors of the article proposed a formal model for assessing the security of the information security management system of a communal complex organization. The developed model uses protection systems with full overlap, which deals with the interaction of the «threat area», the «protected area» (APCS resources) and the «protection system» (security mechanisms of the APCS).The proposed model allows to solve the problem of increasing the security of the APCS of the communal complex organization. The architecture of the software complex for assessing the security of the APCS of the communal complex

organization was developed. The interface, block diagrams of algorithms of the developed program complex are presented. The developed software package has passed test tests at the enterprise of LLC «Kontsessii vodosnabzheniya». The developed software package received the Certificate of state registration of the computer program №2018614780. The test results showed that the application of the software package allowed to increase the security of the APCS of the communal complex organization.

Keywords: information security, information threats, automated process control system, security monitoring, protection mechanisms, security analysis, security evaluation.

Введение

Анализ защищенных диссертационных работ показал широкую распространенность понятия «информационная безопасность» в исследовательской среде. Большая часть научных работ посвящена юридическим аспектам данного понятия: в основном авторы исследуют проблемы «гражданско-правового регулирования» [1-3], «институционального обеспечения информационной безопасности» и других подобных правовых аспектов. Однако, информационную безопасность исследуют с плоскости экономики [4], менеджмента [5], политологии [6] и даже философии [7]. Таким образом, с теоретической точки зрения информационная безопасность не относится к новым и малоисследованным научным категориям. Как отмечается в работе А.В.Дорофеева и А.С.Маркова, под информационной безопасностью (ИБ) обычно понимают «состояние (свойство) защищенности ресурсов информационной системы в условиях наличия угроз в информационной сфере. Защита информации – это процесс, направленный на обеспечение информационной безопасности. Определяющими факторами информационной безопасности являются угроза и риск. Угрозой называют потенциальную причину (событие, нарушение, инцидент), снижающую уровень информационной безопасности системы, т.е. потенциально способную привести к негативным последствиям и ущербу системы или организации» [8]. Риск представляет собой возможный ущерб, как правило, произведение вероятности реализации угрозы и ущерба от нее. Отметим, что угроза и риск определяются не вообще, а относительно конкретного защищаемого ресурса. В терминологии менеджмента бизнес-процессов вместо ресурса используется синонимическое понятие – актив asset, под определение которого подпадает все, что имеет ценность для организации. В информационной сфере примерами активов являются: информация; программное обеспечение; аппаратное обеспечение; информационная система (сложный актив, включающий предыдущие); персонал; имидж организации. В итоге, активами представляются все те объекты,

которые подлежат защите путем выстраивания процессов информационной безопасности» [8].

Проблема информационной безопасности типовой автоматизированной системы управления технологическими процессами организации коммунального комплекса

Под АСУ ТП обычно понимается целостное решение, обеспечивающее автоматизацию основных операций технологических процессов на производстве в целом или каком-то его участке [9]. Составными частями АСУ ТП могут быть отдельные системы автоматического управления (САУ) и автоматизированные устройства, связанные в единый комплекс. Такие как системы диспетчерского управления и сбора данных (SCADA), распределенные системы управления (DCS), и другие более мелкие системы управления (например, системы на программируемых логических контроллерах (PLC)). Функция АСУ ТП – это совокупность действий системы, направленных на достижение частной цели управления. Функции АСУ ТП подразделяются на управляющие, информационные и вспомогательные [10].

На верхнем уровне и уровне корпоративной сети с участием оперативного персонала решаются задачи диспетчеризации процесса, оптимизации режимов, подсчета технико-экономических показателей производства, визуализации и архивирования процесса, диагностики и коррекции программного обеспечения системы. Верхний уровень АСУ ТП реализуется на базе серверов, операторских (рабочих) и инженерных станций.

На среднем уровне – задачи автоматического управления и регулирования, пуска и останова оборудования, логико-командного управления, аварийных отключений и защит. Средний уровень реализуется на основе программируемых логических контроллеров (ПЛК).

Нижний и полевые уровни АСУ ТП обеспечивает сбор данных о параметрах технологического процесса и состояния оборудования, реализует управляющие воздействия. Основными техническими средствами нижнего уровня являются датчики и исполнительные устройства, станции распределенного ввода/вывода, пускатели, концевые выключатели, преобразователи частоты [11].

Для обоснования актуальности исследования, приведем статистическо-аналитические данные от компании Positive Technologies из их отчета «Безопасность АСУ ТП: итоги 2017 года» [12]. Согласно анализу статистики из упомянутого выше источника, 2017 году ощутимо выросло общее количество

выявленных уязвимостей в компонентах АСУ ТП по сравнению с 2016 годом. Лидерами в рейтинге наиболее уязвимых компонентов АСУ ТП являются продукты компаний Schneider Electric, Siemens, Advantech, а также производителя промышленного сетевого оборудования компании Moxa. Основной тренд – рост числа новых уязвимостей в промышленном сетевом оборудовании. Недостатки безопасности были выявлены в продукции Moxa, Hirschmann и PhoenixContact. Если в 2016 году в сетевых устройствах было разглашено в полтора раза меньше уязвимостей, чем в компонентах SCADA/ЧМИ/РСУ5, то по итогам минувших 12 месяцев разрыв сократился до минимума.

К наиболее распространенным типами уязвимостей относятся «Раскрытие информации», «Удаленное выполнение кода» и «Переполнение буфера». В 2016 году два лидера были теми же, а на третьем месте находились уязвимости типа «Отказ в обслуживании».

Анализ структуры информационных потоков автоматизированной системы управления технологическими процессами ООО «Концессии водоснабжения»

Внутри ИС АСУ ТП выделяются следующие информационные потоки (рис. 1):

- информация от датчиков измерения передается к контроллеру;
- от контроллера к устройству магистральной передачи информации (коммутатор, GSM-модуль, радиомодуль);
- от устройства передачи данных к VPN-серверу (опционально);
- от VPN-сервера к SCADA-серверу в локальной сети (опционально);
- от SCADA-сервера информация передается диспетчеру АСУ ТП.

В ИС предприятия используются следующие каналы взаимодействия с внешними сетями:

- выделенный магистральный канал взаимодействия с корпоративной сетью, посредством использования технологии VPN.
- резервная линия связи с сетью Интернет.
- коммутируемый канал связи, посредством использования технологии GPRS.

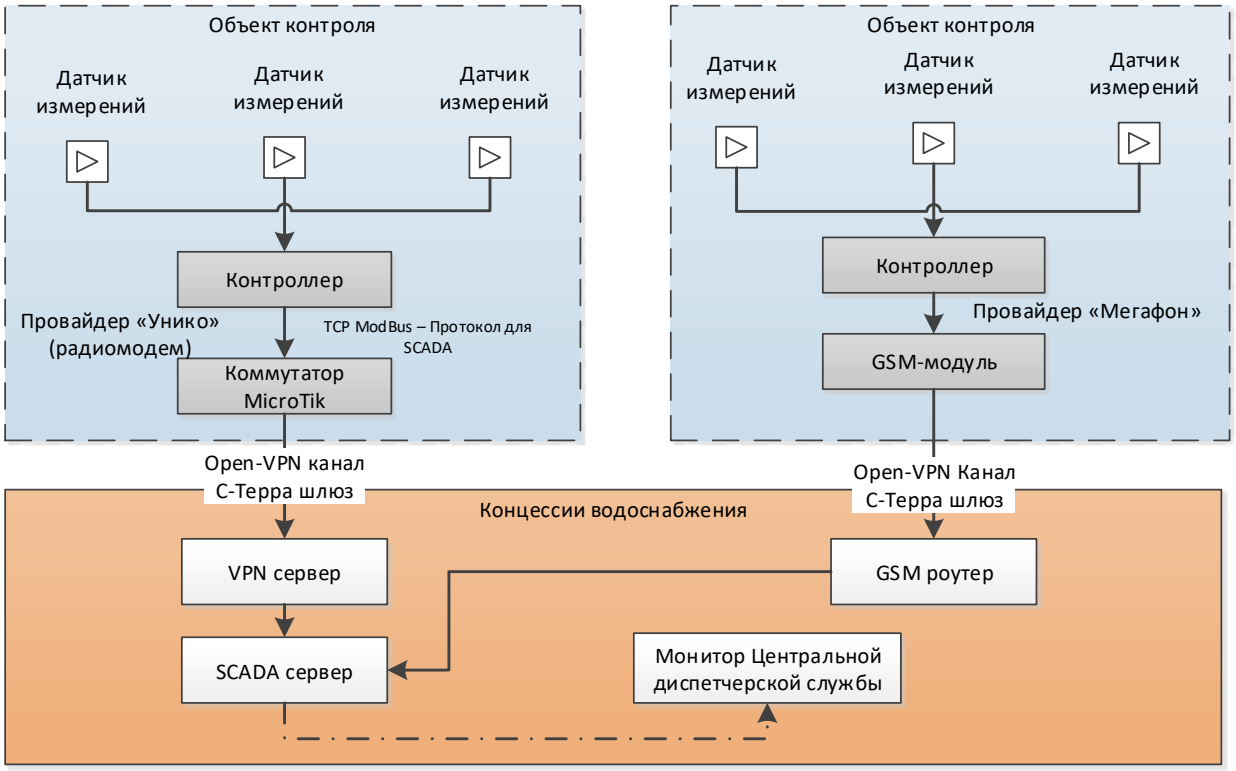

Рисунок 1 – Обобщенная функциональная схема АСУ ТП учета и управления распределением и реализацией воды, внедренной в ООО «Концессии водоснабжения»

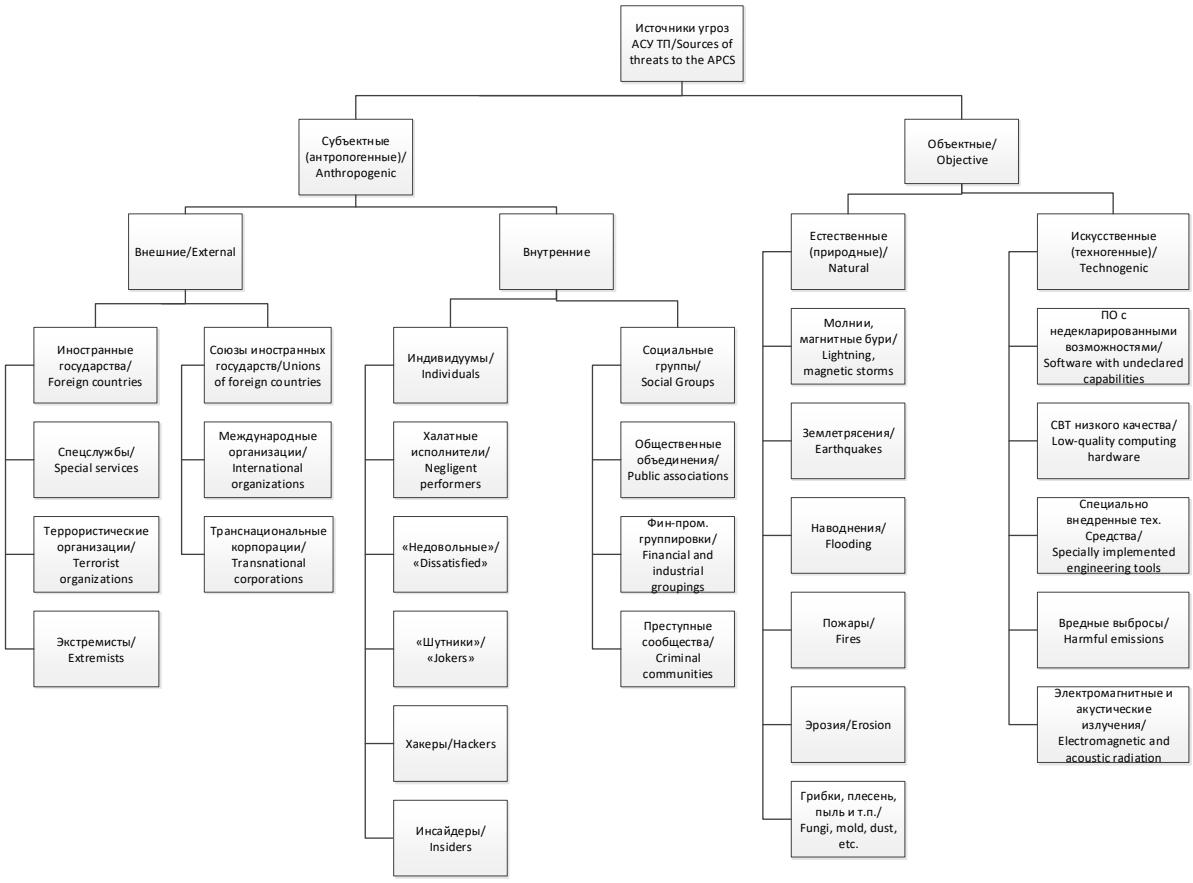

Рисунок 2 – Источники угроз АСУ ТП

Действия вышеизложенных источников угроз могут привести к ряду злоумышленных воздействий и нежелательных последствий, среди которых применительно к АСУ ТП, можно выделить следующие (табл. 1).

Таблица 1 – Классификация злоумышленных воздействий источников угроз АСУ ТП на ВМ АСУ ТП

Источник угрозы АСУ ТП	Действия субъектов при реализации угроз АСУ ТП
Субъектные (антропогенные) источники угроз	
1. Внешние: 1.1. Иностранные государства: 1.1.1. Спецслужбы; 1.1.2. Негосударственные организации; 1.1.3. Граждане иностранных государств; 1.2. Союзы иностранных государств: 1.2.1. Международные организации; 1.2.2. Транснациональные корпорации. 2. **Внутренние**: 2.1. Индивидуумы: 2.1.1. Халатные исполнители; 2.1.2. «Недовольные»; 2.1.3. «Шутники»; 2.1.4. Хакеры; 2.1.5. Инсайдеры. 2.2. Социальные группы: 2.2.1. Общественные объединения; 2.2.2. Финансово-промышленные группировки; 2.2.3. Преступные сообщества.	1) Кража: а) технических средств; б) носителей информации; в) информации; г) средств доступа. 2) Подмена (модификация): а) операционных систем; б) систем управления базами данных; в) прикладных программ; г) информации (данных); д) паролей. 3) Уничтожение (разрушение): а) технических средств; б) носителей информации; в) программного обеспечения; г) информации (файлов, данных); д) паролей и ключевой информации. 4) Нарушение нормальной работы (прерывание): а) скорости обработки информации; б) пропускной способности каналов связи; в) объемов свободной оперативной памяти; г) объемов свободного дискового пространства; д) электропитания технических средств. 5) Ошибки: а) при инсталляции ПО, ОС, СУБД; б) при написании прикладного ПО; в) при эксплуатации ПО; г) при эксплуатации технических средств.
Искусственные (техногенные) источники угроз	
1. ПО с недекларированными возможностями; 2. СВТ низкого качества; 3. Специально внедренные технические средства; 4. Вредные выбросы; 5. Электромагнитные и акустические излучения.	1) Нарушение нормальной работы: а) нарушение работоспособности системы обработки информации; б) нарушение работоспособности связи и телекоммуникаций; в) старение носителей информации и средств ее обработки; г) нарушение установленных правил доступа;

	д) электромагнитное воздействие на технические средства. 2) Уничтожение (разрушение): а) программного обеспечения, ОС, СУБД; б) средств обработки информации (броски напряжений, протечки); в) помещений; г) информации (размагничивание, радиация, протечки и пр.). 3) Модификация (изменение): а) программного обеспечения; б) информации при передаче по каналам связи и телекоммуникациям.
Естественные (природные) источники угроз	
1. Молнии, магнитные бури; 2. Землетрясения; 3. Наводнения; 4. Пожары; 5. Эрозия; 6. Грибки, плесень, пыль и т.п.	Уничтожение (разрушение): а) технических средств обработки информации; б) носителей информации; в) программного обеспечения (ОС, СУБД, прикладного ПО); г) информации (файлов, данных); д) помещений и персонала.

Анализ механизмов защиты АСУ ТП ООО «Концессии водоснабжения» позволил выявить следующие (табл. 2).

Таблица 2 – Анализ механизмов защиты АСУ ТП в ООО «Концессии водоснабжения»

Реализованные механизмы защиты	Рекомендуемые к внедрению механизмы защиты
АнтивирусноеПО «Kaspersky Endpoint Security»	Реализация системы обнаружения вторжений VipNet
OpenVPN	Внедрение межсетевого экрана
«С-Терра Криптошлюз»	Разработка руководящих документов и нормативно-методических документов внутренней политики организации по вопросам ИБ
Резервные каналы связи	Обучение персонала касательно вопросов информационной безопасности
Автоматические регуляторы напряжения	Совершенствование систем видеонаблюдения и СКУД
Резервное копировании данных	Совершенствование систем резервного копирования
Физическая охрана объектов	Внедрение системы автоматического пожаротушения
СКУД (не на всех объектах)	Реализация системы регистрации и аудита событий безопасности
Система видеонаблюдения (не на всех объектах)	
Система пожаротушения	

Формальная модель оценки защищенности автоматизированной системы управления технологическими процессами организации коммунального комплекса

1. Введем три множества:

$X = \{x_j\}$ – множество источников угроз,

$T = \{t_i\}$ – множество угроз безопасности,

$M = \{m_k\}$ – множество механизмов защиты, реализованных и рекомендуемых к внедрению.

O – ресурс АСУ ТП организации коммунального комплекса.

Защищенность АСУ ТП от угроз безопасности S определяется количеством уязвимостей v, для которых в системе не создано барьеров b, перекрывающих эти уязвимости, а также прочностью существующих барьеров [1].

В идеале каждый механизм защиты должен исключать соответствующий путь реализации угрозы t_i. В действительности же механизмы защиты обеспечивают лишь некоторую степень сопротивляемости угрозам безопасности. В связи с этим в качестве характеристик элемента набора барьеров $b_l = <x_j, t_i, m_k>$, может рассматриваться набор $<p_k, l_k, r_k>$, где

P_k – вероятность появления угрозы, которая задается экспертным методом;

L_k – величина ущерба при удачном осуществлении угрозы в отношении защищаемого объекта, которая задается экспертным методом;

R_k – степень сопротивляемости механизма защиты m_k, характеризующаяся вероятностью его преодоления, которая задается экспертным методом.

2. Прочность барьера $b_l = <x_j, t_i, m_k>$ характеризуется величиной остаточного риска $Risk_i$, связанного с возможностью осуществления угрозы безопасности t_i в отношении объекта АСУ ТП, при использовании механизма защиты m_k. Эта величина определяется по формуле:

$$Risk_i = P_k * L_k(1 - R_k) \quad (1)$$

3. Для определения численного значения оценки защищенности S можно использовать следующую формулу:

$$S = \frac{1}{\sum_{k=1}^{n}(P_k * L_k(1 - R_k))}, \quad (2)$$

где n – число угроз, $P_k, L_k \in (0, 1), R_k \in [0, 1)$.

В этой формуле знаменатель определяет суммарную величину остаточных рисков, связанных с возможностью осуществления угроз безопасности T в отношении объекта АСУ ТП, при использовании механизмов защиты M. Суммарная величина остаточных рисков характеризует «общую уязвимость» системы защиты, а защищенность АСУ ТП определяется как величина, обратная ее «уязвимости». При отсутствии в системе барьеров b_k, перекрывающих определенные уязвимости, степень сопротивляемости механизма защиты R_k принимается равной 0.

4. Повышение защищенности ИС выразим формулой:

$$\Delta S = \frac{S_1 + S_2}{S_1}, \quad (3)$$

где S_1 – оценка защищенности ИС с реализованными механизмами защиты; S_2 – оценка защищенности ИС после выполнения рекомендаций по внедрению механизмов защиты.

Предложенное решение и результаты его тестовых испытаний

Формализованная модель позволила разработать архитектуру программного комплекса оценки защищенности АСУ ТП организации коммунального комплекса (рис. 3). Архитектура системы управления реализована на языке C# в виде программного комплекса.

Модуль «Ввод и сохранение исходных данных» предназначен для внесения в хранилище данных и/или извлечения из хранилища данных информации, полученной от пользователя.

Модуль «Вычисление оценки защищенности ИС» предназначен для нахождения численного значения оценки защищенности ИС организации коммунального комплекса с существующими механизмами защиты, а также для вычисления численного значения оценки защищенности ИС организации коммунального комплекса с рекомендуемыми к внедрению механизмами защиты от угроз ИБ.

Модуль «Формирование отчета» служит для нахождения суммы значений оценки защищенности ИС организации коммунального комплекса с существующими и с рекомендуемыми к внедрению механизмами защиты и таким образом отражает повышение защищенности ИС, а также для вывода на экран результата работы программного комплекса.

Хранилище исходных данных служит для хранения введенных пользователем данных, а также для хранения статистических массивов данных.

Пользовательский интерфейс имеет графический вид и предназначен для ввода данных, вывода результатов и организации взаимодействия пользователя с программой.

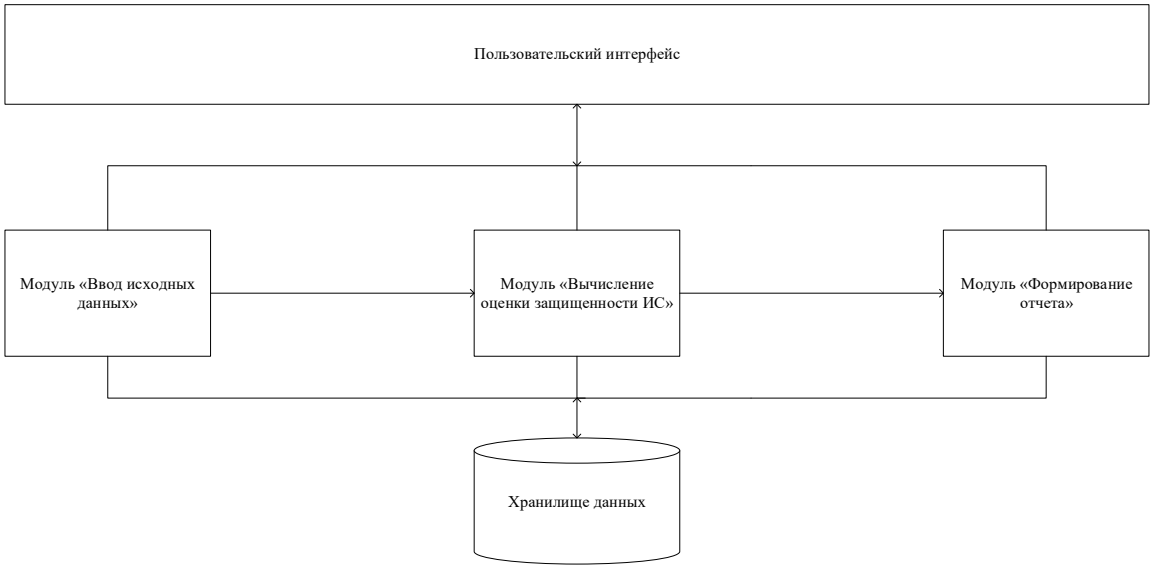

Рисунок 3 – Архитектура программного комплекса оценки защищенности АСУ ТП организации коммунального комплекса

Результаты и обсуждение

С помощью разработанного программного комплекса оценки защищенности автоматизированной системы управления технологическими процессами организации коммунального комплекса были проведены экспериментальные исследования, направленные на повышение защищенности АСУ ТП ООО «Концессии водоснабжения» (рис. 4).

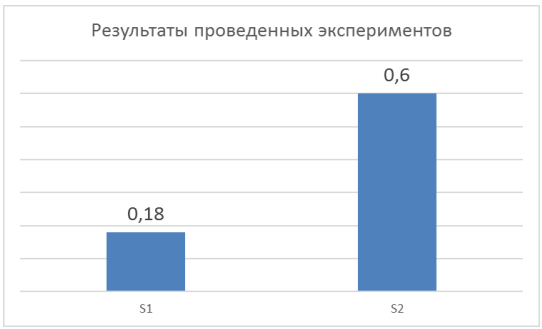

Рисунок 4 – Диаграмма результатов проведения экспериментов: S1 – оценка защищенности АСУ ТП ООО «Концессии водоснабжения» с внедренными механизмами защиты; S2 – оценка защищенности АСУ ТП ООО «Концессии водоснабжения» с рекомендуемыми к применению механизмами защиты

Результаты тестовых испытаний разработанного программного комплекса показали возможность применения данной системы для оценки защищенности АСУ ТП организации коммунального комплекса. Применение данного программного комплекса позволило повысить защищенности АСУ ТП в 4,25 раза.

Заключение

Разработанный программный комплекс оценки защищенности автоматизированной системы управления технологическими процессами организации коммунального комплекса учитывает структуру, компоненты, актуальные угрозы, источники угроз, механизмы защиты, специфику функционирования АСУ ТП предприятия. Программный комплекс, реализующий предложенную модель оценки защищенности, позволяет выбирать актуальные для того или иного предприятия источники угроз, угрозы, а также механизмы защиты ИБ АСУ ТП. По результатам применения программного комплекса подтвержден факт повышения защищенности анализируемой АСУ ТП предприятия. Разработанный программный комплекс может применяться как компонент системы управления информационной безопасностью автоматизированной системы управления технологическими процессами организации коммунального комплекса. Авторы программного комплекса получили Свидетельство о государственной регистрации программы для ЭВМ № 2018614780.

Библиографический список

1. Астахов А. Анализ защищенности корпоративных автоматизированных систем [Электронный ресурс] / А. Астахов // ISO27000.ru. Искусство управления информационной безопасностью : сайт. – Режим доступа: http://iso27000.ru/chitalnyi-zai/audit-informacionnoi-bezopasnosti/analiz-zaschischennosti-korporativnyh-avtomatizirovannyh-sistem.
2. Результаты исследования «Эрнст энд Янг» в области информационной безопасности // Информационная безопасность. – 2010. – № 2. – С. 22–26.
3. Янина Е. В. Гражданско-правовое регулирование информационной безопасности : автореф. дис. … канд. юрид. наук : 12.00.03, 12.00.14 / Е. В. Янина. – Москва, 2004. – 23 с.
4. Андреев П. Г. Институциональное развитие правового обеспечения информационной безопасности в российском информационном праве : автореф. дис. … канд. юрид. наук : 12.00.14 / П. Г. Андреев. – Екатеринбург, 2012. – 23 с.
5. Тютин А. В. Организационно-методический аспект совершенствования подсистемы информационной безопасности объектов промышленного

комплекса региона : автореф. дис. ... канд. экон. наук : 08.00.05 / А. В. Тютин ; Иван. гос. ун-т. – Иваново, 2004. – 23 с.
6. Бубнов А. В. Информационная безопасность России в условиях глобализации : автореф. дис. … канд. полит. наук : 23.00.02 / А. В. Бубнов. – Москва, 2004. –23 с.
7. Цыденова О. М. Философско-этические основания информационной безопасности : автореф. дис. … канд. филос. наук : 09.00.11 / О. М. Цыденова. – Улан-Удэ, 2005. – 23 с.
8. Дорофеев А. В. Менеджмент информационной безопасности: основные концепции / А. В. Дорофеев, А. С. Марков // Вопросы кибербезопасности. – 2014. – № 1 (2). – С. 67–73.
9. КИПиА. Системы автоматического управления [Электронный ресурс] // АВР-ПРОЕКТ : сайт. – Ресурс доступа: http://cc-continent.ru/kipia-sistemy-avtomaticheskogo-upravleniya/.
10. Определение, функции и состав АСУТП [Электронный ресурс] // АСУТП : сайт. – Ресурс доступа: https://automation-system.ru/main/11-asutp/asu-tp/46-41-opredelenie-funkczii-i-sostav-asutp.html.
11. Структура распределённой АСУ ТП [Электронный ресурс] // Teh-Lib.Ru : сб. техн. ст. – Ресурс доступа: http://www.teh-lib.ru/atpip/struktura-raspredeljonnoj-asu-tp/Vse-stranitsy.html.
12. Безопасность АСУ ТП: итоги 2017 года [Электронный ресурс]. – Ресурс доступаhttps://www.ptsecurity.com/upload/corporate/ru-ru/analytics/ICS-Security-2017-rus.pdf.
13. Атаманов Г. А. Источники угроз / Г. А. Атаманов // АГАСОФИЯ : блог Атаманова Г. А. – Режим доступа: http://gatamanov.blogspot.ru/2015/05/blog-post.html.